基于分组密码的跳频序列族构造

李 赞, 常义林, 蔡觉平, 王育民
(西安电子科技大学 ISN 国家重点实验室, 陕西西安 710071)

摘 要: 基于迭代型分组密码的理论体系, 本文从工程实现的角度提出了一种用于跳频码分多址通信系统的新型跳频序列族构造方法. 该算法基于密码学的加密机制, 具有好的安全性和高的计算复杂度; 算法的设计遵循了密码学的"混淆"和"扩散"准则, 生成序列具有各项优异的性能指标. 本文从安全性、随机性、均匀性、复杂度、组网特性及跳频间隔特性等各方面对产生的跳频序列进行了全面的理论分析, 证明该算法具有理想的综合系统性能指标. 在此基础上, 利用 VHDL 语言设计并开发出相应的跳频加密芯片. 经测试其性能稳定、运算速度快、输入方式灵活多样, 已应用于实际的高速跳频通信系统中.

关键词: 分组密码; 跳频序列; 跳频多址接入; VHDL; FPGA
中图分类号: TN914.41 文献标识码: A 文章编号: 0372-2112 (2005) 04-0620-04

Structure of Frequency Hopping Sequences Family Based on Block Cipher

LI Zan, CHANG Yi-lin, CAI Jue-ping, WANG Yu-min
(State Key Lab. of Integrated Services Networks, Xidian Univ., Xi'an, Shaanxi 710071, China)

Abstract: A novel family of frequency hopping sequences based on iterated block cipher is proposed for frequency-hopping multiple-access (FHMA) communications. The design offers a class of nonlinear FH codes with high security, large linear span and a uniform spread over the entire frequency bandwidth. Moreover, FH sequences among the family are independent from each other and they perform as well as random patterns in terms of multiple access interference in anti-jamming applications. With the performance of packet error and throughput for FHMA network being derived in theory, numerical results of the 3DES sequences are presented, comparing with those of shift register sequences and chaotic FH sequences. Efficiently implemented in field-programmable-gate-arrays (FPGA), the generator prototype of the proposed sequence has been realized and incorporated into fast FH radio.

Key words: block cipher; FH sequences; FHMA; VHDL; FPGA

1 引言

跳频通信以其抗干扰、抗衰落、多址性能好及易于与窄带通信系统兼容等特点, 在现代军事通信中得到了广泛的应用. 作为跳频通信的三大关键技术之一, 跳频序列的产生对跳频通信的系统性能有着决定性的影响, 寻求和设计具有理想特性的跳频序列已成为跳频通信的重要课题之一. 现有跳频序列如 m 序列、RS 码序列等[1~4]存在复杂度低等缺点, 不适应战术跳频电台高保密性的要求; 近年来提出的混沌跳频序列[5~8]具有高的计算复杂度, 克服了已有跳频序列的缺点, 其算法实现受有限精度的影响需要引入 m 序列等进行扰动. 本文在现有理论的基础上, 将密码学的加密机制引入到跳频序列的设计当中, 提出了一种新的基于迭代型分组密码的跳频序列族, 使其具有各项优异的性能指标, 并开发出相应的跳频加密芯片, 从而具有实际的应用价值.

2 基于迭代型分组密码构造跳频序列族

2.1 基于分组密码的跳频序列族产生方案

跳频通信中, 系统时钟 TOD(Time Of Day) 和收发信机密钥 KEY 是实现跳频同步的两个重要信息, 跳频系统的 TOD 是共享的且常常用来控制跳频序列的产生, 因此可以作为明文; 收发信机密钥 KEY 用来区分跳频序列以保证数据的正确传输, 可以作为用户密钥. 在此基础上, 可将跳频序列的产生看作密码学的加密问题. 根据 Shannon 提出的针对密码设计的"混淆"(Confusion)和"扩散"(Diffusion)准则, 我们构造了一种基于迭代型分组密码的跳频序列族产生方案, 其计算框图

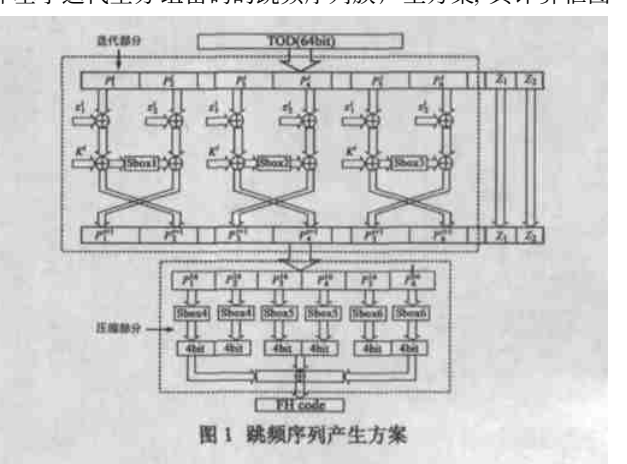

图 1 跳频序列产生方案

收稿日期: 2003-08-01; 修回日期: 2005-01-10
基金项目: 国家自然科学基金(No. 60402040); 国家"十五"军事预研背景课题(No. 020000011001030 3); 国家国防专利授权(No. 00130524.7)

如图 1 所示[9, 10].

图中含义及符号说明如下: (1) 各种计算均以 8bit 为单位, z_1^i, z_2^i 和 K^i 都为 8bit 非负整数, 符号 ⊕表示异或运算; (2) 图中上方的虚线框为轮函数, 其迭代次数为 16 次; (3) K^i 代表第 i 次迭代使用的子密钥, 由输入的用户密钥 KEY 经过循环分割而得到; (4) Sbox1~ Sbox3 为 8bit 输入 8bit 输出的代换盒, Sbox4~ Sbox6 为 8bit 输入 4bit 输出的压缩代换盒. 如图所示, 具体的跳频序列产生方案为: 将输入的 64bit 系统时钟 TOD 划分为 8 个 8bit 子块 P_1, $P_2 \cdots P_6$ 及 Z_1、Z_2, 根据下式进行轮函数的 16 次迭代运算, 即

$$\begin{cases} P_{2j}^{i+1} = P_{2j-1}^{i} \oplus K^i \oplus z_1^i \\ P_{2j-1}^{i+1} = Sbox j(P_{2j}^{i+1}) \oplus P_{2j}^{i} \oplus z_2^i \end{cases}, \quad j = 1, 2, 3 \quad i = 1, 2, \cdots, 16 \quad (1)$$

其中 i 为迭代次数, 且

$$z_n^i = \begin{cases} Z_n, & i = 8, 16 \\ 0, & \text{others} \end{cases}, \quad i = 1, 2, \cdots 16, \ n = 1, 2 \quad (2)$$

迭代之后进行压缩运算, 进而得到明文 TOD 对应的生成密文 C, 即 $C = \{Sbox4(P_2^{16}) \oplus Sbox5(P_4^{16}) \oplus Sbox6(P_6^{16})\} + \{Sbox4(P_1^{16}) \oplus Sbox5(P_3^{16}) \oplus Sbox6(P_5^{16})\} \lll 4$ (3)

式中≪为循环左移运算符. 对可用频隙数为 $q = 2^n$ ($n = 1, 2, \cdots, 8$) 的跳频系统, 选取生成密文 C 中的固定 n 比特 $\{c_1, c_2, \cdots, c_n\}$ 作 TOD 时刻对应的跳频码, 即 $f(TOD) = \sum_{i=1}^{n} c_i 2^{n-i}$.

2.2 跳频序列性能分析及仿真

如前所述, 上述的跳频序列产生算法基于迭代型分组密码的加密机制, 经过若干轮迭代使“扩散”和“混淆”的准则得以充分满足, 因而产生的跳频序列具有优异的综合性能指标. 由于分组密码性能的理论分析难以获得[11], 我们从统计检验的角度进行分析和仿真:

2.2.1 安全性 跳频序列的安全性取决于作为方案基础的分组密码体制的安全性. 该体制中, Sbox 是唯一的非线性因素, 它的性能好坏是分组密码安全性的重要指标. Sbox 具有高度非线性、鲁棒性、强雪崩效应及输入输出差分近似等概性等性质, 使该分组密码具有很好的抗差分攻击能力[11]. 实际通信中, 由于无法获得完整的明密文, 而难以发动已知明文攻击和选择明文攻击, 且采用密钥穷尽法攻击该分组密码的复杂度为 (2^{64}). 因此, 我们认为该方案是安全的.

2.2.2 均匀性 为了增强抗干扰能力和提高组网性能, 要求跳频序列在频带内均匀分布, 这就是均匀性问题. 好的均匀性能够使各载波被等概率的选取, 从而提高系统的抗电磁干扰能力. 这里, 我们采用标准的 chi squared 检验, 即 χ^2 检验法来检验衡量跳频序列的均匀性程度. 我们假设 H_0: 跳频序列是均匀分布的, 根据 Pearson 定理使用统计量

$$\chi^2 = \sum_{t=1}^{k} \frac{[\text{num}(X_t) - NP_t]^2}{NP_t} \quad (4)$$

作为检验假设 H_0 与实际符合程度的尺度. 在观测长度 N 充分大 ($N \geqslant 50$) 的情况下, 统计量服从自由度为 $k - r - 1$ 的 χ^2 分布, 若 $\chi^2 < \chi^2_{(k-r-1);\alpha}$ 则在水平 α 下接受 H_0. 均匀性检验可分成两类: (1) 等分布检验: 跳频序列中各频隙出现的概率密度应该均匀且 $P_t = 1/q$, $\text{num}(X_t)$ 为跳频序列 $\{f_i\}$, $i = 1, 2, \cdots N$ 中频隙 f_t, $t \in (1, 2, \cdots q)$ 出现的次数, 则估计参数 $r = 0$, $k = q = 2^6$ 时 H_0 成立置信度为 0.05 的肯定域为 $\chi^2_{(k-r-1);\alpha} = \chi^2_{(63);0.05} = 82.2447$; (2) 连续性检验: 跳频序列各对连续字的概率密度应该均匀且 $P_t = 1/q^2$, $\text{num}(X_t)$ 为跳频序列 $\{f_i\}$, $i = 1, 2, \cdots N$ 中各对连续频隙出现的次数, 则估计参数 $r = 0$, $k = q^2 = 64^2$ 时 H_0 成立的置信度为 0.05 的肯定域为 $\chi^2_{(k-r-1);\alpha} \approx (z_\alpha + \sqrt{2n-1})^2/2 = 4244.7$. 通过多次统计, 选择不同的用户密钥和起始 TOD, 得到观测长度 $N = 2^{16}$ 的 χ^2 值绝大部分都落入此范围内 (部分统计结果见表 1), 所以在显著水平 0.05 下接受原假设 H_0, 即基于分组密码的跳频序列是均匀分布的.

表 1　均匀性检验结果

字组	TOD	KEY	等分布检验	连续性检验
			χ^2	
1	000000	ACBCD21 14DAE1577	65.0078	4046.0
2	000000	C6DBF4C91A3CDA2F	71.7813	3943.8
3	0001	169B340989C1D32C	65.7891	4000.3
4	14E6F	ACBCD21 14DAE1577	75.3281	4100.0
5	3BB00	C6DBF4C91A3CDA2F	71.6641	4036.3
6	000001	169B340989C1D32C	60.9590	3860.8
7	3A019	ACBCD21 14DAE1577	61.4980	3985.3
8	432002	C6DBF4C91A3CDA2F	74.0293	4091.3
9	0BA38	169B340989C1D32C	68.5820	4145.0

2.2.3 随机性 随机性检验又称为独立性检验, 它用来检验两个随机变数之间的统计相关性是否显著. 好的随机性能够保证跳频码具有不可递推性, 理想的伪随机序列应有类似于高斯白噪声的性能. 通过对任意跳频序列 $F_0 = \{f_0, f_1, f_2, \cdots\}$ 及其移位序列 $F_i = \{f_{0+i}, f_{1+i}, f_{2+i}, \cdots\}$ ($i = 1, 2, \cdots, 500$) 进行 10 次计算平均来检验其随机性. 为了便于比较, 图 2 给出了在自由度为 $(q-1)^2 = 255^2$ 时, 基于分组密码的跳频序列、M 跳频序列及 1σ gistic 映射的混沌跳频序列[5, 7]的 χ^2 检验结果. 可以看出, 混沌序列的值具有很大的起伏, 而本文所提的序列和 M 跳频序列的 χ^2 值相对稳定, 且其 95% 以上的观测点样值均小于 65604.56191 即满足式 (5), 因此说明序列具有较强的独立性.

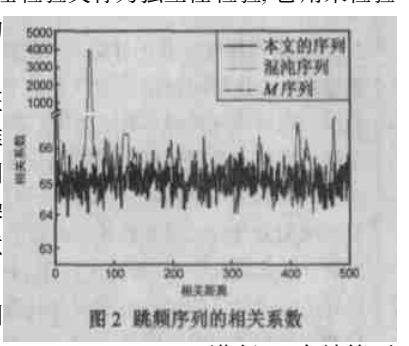

图 2 跳频序列的相关系数

$$prob(\chi^2 > 65604.56191) = 0.0543 \quad (5)$$

2.2.4 线性复杂度 线性复杂度直接决定了跳频序列的抗破译能力. 随机序列的复杂度定义为产生该序列的等效线性反馈移位寄存器 (LFSR) 的最小级数, 可由 Massey 算法[12] 确定. 对于二进制的跳频序列而言, 周期为 $r^L - 1$ 的 m 序列的复杂度仅为移位寄存器级数 L; M 序列引入非线性运算, 复杂度大于 m 序列. 根据前面的分析可知, 基于分组密码的跳频序列是独立、均匀分布的贝努利随机序列, 因此其线性复杂度的均值约为序列观测长度的 1/2[13], 具有理想的线性复杂度特

性, 仿真结果及比较见表 2.

表 2 跳频序列的计算复杂度

	比特数	$N=200$	$N=400$	$N=600$	$N=800$	$N=1000$
本文所提序列	6bits	100	198	299	397	498
	8bits	99	200	299	399	497
混沌跳频序列	6bits	98	197	298	398	498
	8bits	99	199	299	397	499
M 跳频序列	6bits	13	13	13	13	13
	8bits	138	138	138	138	138

注: N 为跳频序列的观测长度

2.2.5 跳频间隔 跳频通信常常希望跳频序列满足宽间隔跳频的要求, 即相邻跳频时隙里发射的两个载波的频率间隔大于某规定值 D, 从而增强系统的抗干扰和抗多径衰落能力, 实现频率分集. 我们定义 $d=|f_{i+1}-f_i|$, 由于$\{f_i\}$是贝努利随机序列, 则跳频间隔分布为[8]

$$P(d=k)=\begin{cases}1/q, & k=0\\ 2(q-d)/q^2, & 1\le k\le q-1\end{cases} \tag{6}$$

跳频间隔的均值是 $$E(d)=(q^2-1)/3q\approx q/3 \tag{7}$$

跳频间隔小于某一规定值 D 的概率为

$$P(d\le D)=\frac{2D+1}{q}-\frac{D(D+1)}{q^2} \tag{8}$$

可见, 频点数 q 越大此概率值越小. 在实际的宽间隔系统要求下, 若$|f_{i+1}-f_i|\le D$ 则可在密文C 中另外选取固定的 n 个比特表示频率号. 仿真结果表明, 在 $q=2^7$, $D=2$ 的条件下此概率小于 7×10^{-5}.

2.2.6 组网特性 基于分组密码的跳频序列产生算法中, 初始输入一个比特的变化就会改变整个输出的结果, 因此该序列族的跳频序列数即可容纳的用户数为 2^{64}个, 完全满足跳频组网的多用户要求. 目前, 跳频码分多址(FHMA)已成为跳频组网研究的热点, 跳频序列的性能直接决定着跳频系统的多址组网能力. 然而, 现有的各类跳频序列产生方法没有对这方面进行深入研究[1~8]. 我们在建立 FHMA 组网模型的基础上推导了跳频网络的误分组率和吞吐量性能, 并通过系统仿真检验了跳频序列的组网能力. 不失一般性, 构造典型的跳频组网完全随机多址接入模型, 如图 3 所示. 设跳频网络中有 $K(K\ge2)$ 个用户同时发送分组数据, f_m^k ($k=1,2,\cdots,K$; $m=1,2,\cdots,M$) 表示第 k 个用户在一个数据分组内第 m 个频率点的跳频码, 其中 M 为每一分组传输所占用的频点数. 则任一用户 k 成功传送一个数据分组的概率为

图 3 跳频组网的系统模型

$$P_r(M,K,q)=(1-q^{-1})^{M(K-1)} \tag{9}$$

误分组率为 $$P_e(M,K,q)=1-P_r(M,K,q) \tag{10}$$

在此基础上, 可以进一步得出 $K\gg1$ 的情况下跳频网络正确传输的业务量即吞吐量 S 和吞吐效率 η 分别为

$$S\overset{K\gg1}{=}\sum_{k=1}^{\infty}kP_r(M,k,q)p(k)\approx Ge^{-G(M/q)} \tag{11}$$

$$\eta(M,q,G)\overset{K\gg1}{=}e^{-G[1-(1-q^{-1})^M]}\approx e^{-G(M/q)} \tag{12}$$

其中 $p(k)$ 为分组数据到达的分布概率密度, G 为跳频系统的总业务量. 根据式(9)和(11)分别作出分组数据正确传输概率和跳频网络吞吐量的理论曲线及跳频序列的仿真曲线, 并与现有混沌跳频序列[5,7]相比较, 如图 4 和图 5 所示. 可以看出, 仿真曲线很好的逼近了理论曲线且优于混沌跳频序列, 从而证明该序列具有近似理想的组网特性.

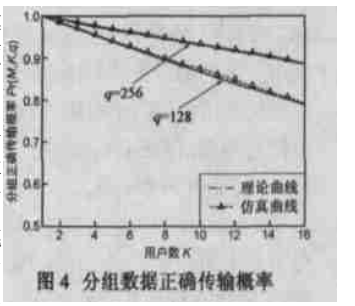

图 4 分组数据正确传输概率

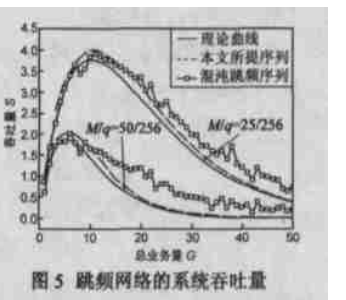

图 5 跳频网络的系统吞吐量

3 跳频加密芯片的设计实现

对上述基于分组密码的跳频序列产生算法进行硬件开发, 使其具有实用性. 采用 VHDL 语言有限状态机的方法[14,15], 自顶向下的进行系统的模块化设计. 整个硬件结构包括时序电路和组合电路, 是以系统输入时钟为基准的同步电路. 根据算法流程将整个硬件电路划分为接收(Receive)、计数器(Counter_64)、核心处理(Process)及压缩(Compress)四大顶层功能模块, 模块之间的关系如图 6 所示. 在总体设计中, 敏感信号线控制状态机的转移, 从而控制和启动不同的运算模块共同协调完成系统功能, 跳频加密芯片的顶层状态转移如图 7. 对于每个功能模块的具体开发设计, 同样使用有限状态机的方法进行子模块的进一步划分, 通过状态机的逐层嵌套和相互调用关系, 最终实现跳频加密芯片的各项功能.

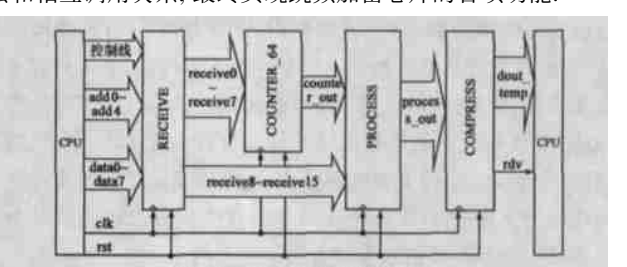

图 6 跳频加密芯片的硬件结构

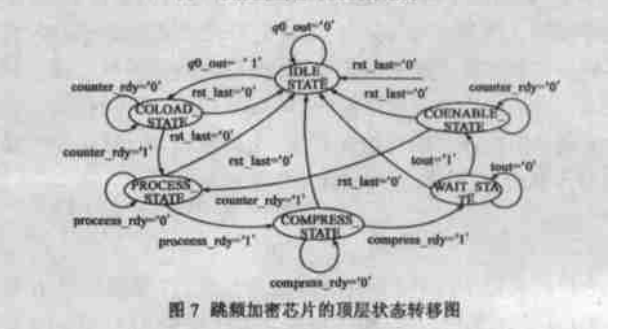

图 7 跳频加密芯片的顶层状态转移图

实现中选用 Altera 公司 144 pin TQFP 封装的 FLEX10K20 进行 VLSI 开发, 设计实现指标见表 3. 实现的跳频加密芯片在

系统时钟为 1.5MHz 时的功耗电流为 10mA, 可以用于手持跳频通信系统.

设计实现的跳频加密芯片经系统测试, 具有以下特点:

(1) 性能稳定, 冗余度大. 对于系统给定的 1.5MHz, 3MHz …24MHz 时钟, 芯片均能满足 1032 跳/秒的高速跳频通信要求. 对于给定时钟范围以外的部分时钟频率也进行了测试, 该芯片同样能够稳定工作, 适应各类跳频通信系统的工作时钟, 冗余度大.

(2) 运算速度快. 使用逻辑分析仪对跳频加密芯片的运算速度进行了测试, 输出延迟仅为 FPGA 芯片固有的门级延迟 17ns, 表明该芯片具有运算速度快的优点, 能够满足高速、超高速跳频电台的要求. 具体测试结果见表 4.

表 3　跳频加密芯片的设计实现指标

系统时钟	1.5MHz
最大跳速	23850hops/s
跳频时刻 TOD	64bits
用户密钥	144bits
可用频点数	2^n (n = 1, 2, …16)

表 4　跳频加密芯片的运算速度

系统时钟(MHz)	运算时间(μs)
1.5	35.18
3	17.50
6	8.65
12	4.38
24	2.15

(3) 输入方式灵活多样. 实际通信中, CPU 常常需要实时更换 TOD 以重新初始化系统, 或更换用户原始密钥以确保通信的安全可靠. 跳频加密芯片中 TOD 与原始密钥按地址分别存储, 因此 CPU 既可以随时按需要进行初始化输入, 又可以根据实际情况随时按地址改变其中的值, 即进行一般输入具有很大的输入灵活性.

(4) 可移植性强. 该芯片使用硬件电路自顶向下的模块化设计方法, 将整个系统划分为几个功能模块, 每个功能模块独立完成一个特定的功能, 模块之间的接口简单明确, 易于相互之间以及与其它硬件电路的联接. 该芯片采用 VHDL 硬件描述语言设计, 容易修改, 可移植性强.

4　结论

本文从工程实现的角度, 将密码学的加密机制引入到跳频序列的设计之中, 提出了一种新的基于迭代型分组密码的跳频序列产生方案. 通过对生成跳频序列的各项性能指标进行了理论分析和仿真, 证明其具有较理想的综合性能指标. 在此基础上, 利用 VHDL 语言有限状态机的设计方法, 在 ALTERA FELX10K20 上开发出的跳频加密芯片性能稳定、运算速度快、输入方式灵活, 可广泛应用于高速、超高速跳频电台. 目前, 该芯片已应用于 1032 跳/秒的高速跳频通信系统中, 并投入批量生产和使用.

参考文献:

[1] Mei Wenhua, Yang Yixian. Families of FH sequences based on pseudo-random sequences over GF(p)[J]. ICCT2002, 1(5): 536–538.

[2] F M D A. Hit probability between frequency hopping sequences generated by Reed-Solomon and Hermitian codes[J]. Electronics Letters, 1996, 32(11): 962–963.

[3] 汪海洋, 等. 重构 L-G 模型及改进模型跳频序列[J]. 通信学报, 2003, 24(1): 98–103.
Wang Haiyang, et al. Reproducing algorithm of Lempel-Greenberger sequence and improved model in hopping frequency[J]. Journal of China Institute of Communications, 2003, 24(1): 98–103(in Chinese).

[4] Seong-Bok Park, K wang-Eog Lee, Young-Kyun Choi. Some good frequency hopping sequences with arbitrary number of slots[J]. IEEE Military Communications Conference MILCOM, 2001(2): 1325–1329.

[5] Ling Cong, Wu Xiaofu. Design and realization of an FPGA-based generator for chaotic frequency hoping sequences[J]. IEEE Trans Circuits and Syst. I, 2001, 48(5): 521–532.

[6] Hongxia Wang and Juebang Yu. A new cipher quasi-chaotic frequency hopping sequence for FH/CDMA communications[A]. IEEE International Conference on Communications, Circuits and Systems and West Sino Expositions[C]. 2002. 497–501.

[7] 凌聪, 孙松庚. 用于跳频码分多址的混沌跳频序列[J]. 电子学报, 1999, 27(1): 67–69.
Ling Cong, Sun Songgeng. Frequency-hopping sequences by chaotic maps for FH/CDMA communications[J]. Acta Electronica Sinica. 1999, 27(1): 67–69(in Chinese).

[8] 邓洪敏, 何松柏, 虞厥邦. 基于一种特定混沌映射的跳频系统[J]. 系统工程与电子技术, 2002, 24(10): 45–46.
Deng Hongmin, He Songbai, Yu Juebang. A frequency-hopping system based on a specific chaotic map[J]. Systems Engineering and Electronics, 2002, 24(10): 45–46(in Chinese).

[9] Zan Li, Yilin Chang, Lijun Jin. A novel family of frequency hopping sequences for multi-hop bluetooth networks[J]. IEEE Trans Consumer Electronics, Nov. 2003, 49(4): 1084–1089.

[10] Zan Li, Yilin Chang, Lijun Jin, Jueping Cai. Analysis of FHMA performance on block cipher based frequency hopping sequences[J]. IEEE Communications letters, July 2004, 8(7): 434–436.

[11] 王育民, 刘建伟. 通讯网的安全-理论与技术[M]. 西安: 西安电子科技大学出版社, 1999. 126–152.

[12] James L. Massey. Shift-register synthesis and BCH decoding[J]. IEEE Trans Information theory, 1969, IT-15(1): 122–127.

[13] R A Rueppel. Analysis and Design of Stream Ciphers[M]. New York: Springer-Verlag, 1986.

[14] Kuusilinna K, et al. Finite state machine encoding for VHDL synthesis[J]. IEE Proceedings: Computers and Digital Techniques, 2001, 148(1): 23–30.

[15] Bolchini C, Montandon R, et al. Design of VHDL-based totally self-checking finite-state machine and data-path descriptions[J]. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2000, 8(1): 98–103.

[16] R K Morrow. Packet throughput in slotted Aloha DS/SSMA radio systems with random signature sequences[J]. IEEE Trans on Communartion, 1992, 40(7): 1223–1230.

作者简介:

李　赞　女, 1975 年出生于陕西省西安市, 现为西安电子科技大学军事通信学副教授, 硕士生导师. E-mail: zanli@xidian.edu.cn.

常义林　男, 1944 年出生于江苏省扬州市, 现为西安电子科技大学通信与信息系统教授, 博士生导师. E-mial: ylchang@xidian.edu.cn.